MASTER OF SCIENCE
IN
COMPUTER SCIENCE

A FRAMEWORK FOR MAXIMIZING THE SURVIVABILITY OF NETWORK DEPENDENT SERVICES

Baris Aktop-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1997
Master of Science in Computer Science-March 2003
Advisor: Geoffrey Xie, Department of Computer Science
Second Reader: John Gibson, Department of Computer Science

As a consequence of the developments in information technology and the Internet, the world is getting increasingly dependent upon distributed systems and network services. Unfortunately, the security of these services has not kept pace with the advances in information technology itself. Security practitioners accept that a system that is connected to an unbounded network, e.g., the Internet, will be vulnerable to attacks regardless of its security features. However, the emerging discipline of survivability can help ensure that such systems deliver essential services and maintain essential properties, such as integrity, confidentiality and performance, despite the presence of intrusions.

Although survivability has been accepted as a means of sufficiently addressing the security problems of current network services, unfortunately, the studies that have been done on network survivability so far are not mature enough and they lack quantifiable metrics.

To address this lack of network survivability measure, a global connectivity metric is developed in this thesis. Additionally, an election protocol based on this metric is designed for the SAAM prototype to enhance the survivability of the SAAM server.

KEYWORDS: SAAM Survivability, SAAM Security, Survivability, Security, Survivability Metric, Edge-disjoint Paths, Java Implementation of Finding Maximum Number of Edge-disjoint Paths

COMPUTER WIRELESS NETWORKS: A DESIGN PLAN FOR BUILDING WIRELESS NETWORKS USING IEEE 802.11 STANDARD

Hamed Almantheri-Royal Army of Oman
B.S., Embry-Riddle Aeronautical University, 1986
Master of Science in Computer Science-March 2003
Advisor: Bert Lundy, Department of Computer Science
Second Reader: Richard Riehle, Department of Computer Science

In spite of the fact that wireless network technology has been available for long period of time, there has been very limited wireless networks deployments around the world before 1997 due to the lack of a widely recognized standard for wireless networks. Thanks to the approval of the IEEE 802.11 family of standards in 1997, the world has witnessed tremendous deployment and proliferation of wireless networks in all aspects of life.

Although the IEEE 802.11 family of standards has been ratified to design radio transceivers for wireless computer stations capable of interconnecting with other wireless computer stations in close proximity, the technology has been successfully employed to design and implement wireless networks with a greater number of distant wireless computer stations with reasonable data throughput and flexibility.

This thesis explores wireless network technology and the primary building blocks and components of a wireless network. It also explores the IEEE 802.11 standard and its technical specifications including the Physical layer (PHY), the Media Access Control layer (MAC), and the ongoing task forces. Additionally, the thesis examines wireless network security, including vulnerabilities, ongoing improvements, and recommendations. Next, it investigates the market for available wireless devices compatible with the IEEE

802.11 standard that can be used to build a wireless network with high data throughput and a high level of security.

Subsequently, the thesis formulates a design plan for a civilian wireless network with different scenarios in order to provide a speedy solution to the limited broadband service availability in the Sultanate of Oman. Additionally, the thesis formulates a generic design plan for a military wireless network with different scenarios that can be rapidly deployed in the field of operations.

KEYWORDS: IEEE 802.11, Media Access Control Layer, Physical Layer, Wireless Local Area Network, Wireless Point of Presence, Hotspots, WPOP, Hotspots, Access Point, Wireless Network Interface Card, Wireless Router

AN EVALUATION OF BEST EFFORT TRAFFIC MANAGEMENT OF SERVER AND AGENT-BASED ACTIVE NETWORK MANAGEMENT (SAAM) ARCHITECTURE

Birol Ayvat-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1997
Master of Science in Computer Science-March 2003
Advisor: Geoffrey Xie, Department of Computer Science
Second Reader: John Gibson, Department of Computer Science

The Server and Agent-based Active Network Management (SAAM) architecture was initially designed to work with the next generation Internet, where increasingly sophisticated applications will require QoS guarantees. Although such QoS traffic is growing in volume, Best Effort traffic, which does not require QoS guarantees, needs to be supported for the foreseeable future. Thus, SAAM must handle Best Effort traffic as well as QoS traffic.

A Best Effort traffic management algorithm was recently developed for SAAM to take advantage of the abilities of the SAAM server. However, this algorithm has not been evaluated quantitatively.

This thesis conducts experiments to compare the performance of the Best Effort traffic management scheme of the SAAM architecture against the well known MPLS Adaptive Traffic Engineering (MATE) algorithm. A couple of realistic network topologies were used. The results show that while SAAM may not perform as well as MATE with a fixed set of paths, using SAAM's dynamic path deployment functionality allows the load to be distributed across more parts of the network, thus achieving better performance than MATE. Much of the effort was spent on implementing the MATE algorithm in SAAM. Based on the experimental results, some modifications were also made to the SAAM code to increase the performance of SAAM's Best Effort solution.

KEYWORDS: Next Generation Internet, Quality of Service, Best Effort Traffic, Networks, Routing, Resource Management

AUTONOMOUS AGENT-BASED SIMULATION OF AN AEGIS CRUISER COMBAT INFORMATION CENTER PERFORMING BATTLE GROUP AIR-DEFENSE COMMANDER OPERATIONS

Sharif H. Calfee-Lieutenant, United States Navy
B.S., United States Naval Academy, 1996
Master of Science in Computer Science-March 2003
Advisors: Neil C. Rowe, Department of Computer Science
John Hiles, Department of Computer Science

The AEGIS Cruiser Air-Defense Simulation is a program that models the operations of a Combat Information Center (CIC) team performing the ADC duties in a battle group using Multi-Agent System (MAS) technology implemented in the Java programming language. Set in the Arabian Gulf region, the simulation is a top-view, dynamic, graphics-driven software implementation that provides a picture of the CIC team grappling with a challenging, complex problem. Conceived primarily as a system to assist ships, waterfront training teams, and battle group staffs in ADC training and doctrine formulation, the simulation was designed to gain insight and understanding into the numerous factors (skills, experience, fatigue, aircraft numbers, weather, etc.) that influence the performance of the overall CIC team and watchstanders. The program explores the team's performance under abnormal or high intensity stress situations by simulating their mental processes, decision-making aspects, communications patterns, and cognitive attributes. Everything in the scenario is logged, which allows for the reconstruction of interesting events (i.e. watchstander mistakes, chain-of-error analysis) for use in post-scenario training as well as the creation of new, more focused themes for actual CIC team scenarios. The simulation also tracks various watchstander and CIC team performance metrics for review by the user.

KEYWORDS: Battle Group Air-defense, Multi-agent Systems, Artificial Intelligence, Air-defense Commander, Naval Simulations, Combat Information Center, Air-defense Simulation, AEGIS, Cruiser, CG, Human-computer Interface (HCI), Watchstander Training, Naval Air Defense, Threat Assessment, Decision Making, Cognitive Factors, AEGIS Doctrine, Air-defense Doctrine, Interactive Training Systems, Watchstander Fatigue, Link-16/TADIL J, Link-11/TADIL A, *USS VINCENNES*

DETERMINE NETWORK SURVIVABILITY USING HEURISTIC MODELS

Eng Hong Chua-Civilian, Defence Science and Technology Agency, Singapore
B.E., Nanyang Technological University, 1998
Master of Science in Computer Science-March 2003
Advisor: Geoffrey Xie, Department of Computer Science
Second Reader: Bert Lundy, Department of Computer Science

Contemporary large-scale networked systems have improved the efficiency and effectiveness of our way of life. However, such benefit is accompanied by elevated risks of intrusion and compromise. Incorporating survivability capabilities into systems is one of the ways to mitigate these risks.

The Server Agent-based Active Network Management (SAAM) project was initiated as part of the next generation Internet project to address increasing multi-media Internet service demands. Its objective is to provide a consistent and dedicated quality of service to users. SAAM monitors the network traffic conditions in a region and responds to routing requests from the routers in that region with optimal routes. Mobility has been incorporated to the SAAM server to prevent a single point of failure from bringing down the entire SAAM server and its service.

With mobility, it is very important to select a good SAAM server locality from the client's point of view. The choice of the server must be a node where connection to the client is most survivable. In order to do that, a general metric is defined to measure the connection survivability of each of the potential server hosts.

However, due to the complexity of the network, the computation of the metric becomes very complex too. This thesis develops heuristic solutions of polynomial complexity to find the hosting server node. In doing so, it minimizes the time and computer power required.

KEYWORDS: Fault Tolerance, Network, Reliability, Survivability, Server Placement

SPEEDING UP A PATH-BASED POLICY LANGUAGE COMPILER

Ahmet Guven-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1997
Master of Science in Computer Science-March 2003
Advisors: Geoffrey Xie, Department of Computer Science
Neil C. Rowe, Department of Computer Science

A new policy language, Path-based Policy Language (PPL), was recently developed. It encompasses as many of the features addressed in the other policy languages as possible, as well as providing means for testing policies for consistency and defining both static and dynamic policies. Most importantly, PPL provides the ability to detect and resolve conflicts by translating policy rules into formal logic statements and checking them with a Prolog program. Even though in theory PPL seems to be a very high performance policy language, its current compiler has a performance bottleneck. In some cases, the PPL compiler can not finish compilation and runs forever without returning any conflict results. This thesis focuses on the

PPL compiler's performance bottleneck and introduces solutions speeding up the PPL compiler. The new PPL compiler achieves a reasonable compilation time for any configuration file for a network with 100 nodes, while maintaining its ability to detect and resolve policy conflicts.

KEYWORDS: Policy, Policy Language, Path-based Policy Language, Compiler, Conflict, Conflict Detection, Conflict Resolution, Prolog, Articulation Point, Biconnected Components, Depth Limited Bidirectional Search

ANALYZING ANTI-TERRORIST TACTICAL EFFECTIVENESS OF PICKET BOATS FOR FORCE PROTECTION OF NAVY SHIPS USING X3D GRAPHICS AND AGENT-BASED SIMULATION

James Harney-Lieutenant, United States Navy
B.S., United States Naval Academy, 1996
Master of Science in Computer Science-March 2003
Advisors : Don Brutzman, Department of Information Science
Curtis L. Blais, Modeling, Virtual Environments, and Simulation Institute
John Hiles, Modeling, Virtual Environments, and Simulation Institute
Gordon Schacher, Emeritus Professor of Physics

Despite the many advances achieved within both modeling and simulation and information technology over the past several decades, practical application of such technology remains under-utilized by operational units in the United States Navy. Furthermore, when such technology has been deployed in the last decade it has been to exercise operator proficiency or increase C4I battlespace awareness. Few tools have allowed operational warfighters to run "what-if" simulation scenarios to aid in development of tactical plans for executing published doctrine.

The approach taken in this thesis is to select an exemplar warfare area, in this case Anti-terrorism and Force Protection for Navy ships, and through research and development, to identify, develop, and deploy the necessary modeling and simulation (M&S) technologies to demonstrate a prototypical planning tool that can be used by today's deployed warfighter. All research and work is conducted in a web-based, "user-centric" fashion utilizing a combination of user-driven and agent-based control of entities for simulation iterations, along with various open source technologies which include Extensible 3D Graphics (X3D), Scalable Vector Graphics (SVG), and Extensible Markup Language (XML). Conventions are demonstrated for the integration of the many academic disciplines utilized during this research to achieve automatic generation of tactically significant scenarios. In order to give the end-user the greatest insight towards potential drawbacks in the tactical planning against surface-borne terrorist threats, various 2D and 3D media provide both real-time and non-real time scenario playback.

The result of this work is a fully integrated, prototypical, Java-based application that demonstrates how various open-source, web-based technologies can be applied in order to provide the tactical operator with tools to aid in Force Protection planning. Scenarios can be auto generated, viewed, analyzed, and manipulated by end users with little to no computer experience necessary beyond requirements for operation of a desktop personal computer (PC) in the Information Technology for the 21st Century (IT-21) environment at sea. This approach has broad applicability to improve the tactical awareness and defensive posture of ships defending against terrorist attacks in port.

KEYWORDS Virtual Environments, Extensible 3D Graphics, X3D, Scalable Vector Graphics, SVG, Force Protection, Anti-terrorism, Extensible Markup Language, XML, Java, Scenario Generation, DIS-Java-VRML, Extensible Modeling and Simulation Framework (XMSF), SAVAGE, Distributed Interactive Simulation, NPSNET-V

TOWARDS AN INTEROPERABILITY ONTOLOGY FOR SOFTWARE DEVELOPMENT TOOLS

Neji Hasni-Lieutenant, Tunisian Navy
B.S., Tunisian Naval Academy, 1989
Diplôme d'Étude Approfondi, Tunisian Naval Academy, 1995
Master of Science in Computer Science-March 2003
Advisors: Man-Tak Shing, Department of Computer Science
LTC Joseph Puett, USA
Second Reader: Richard Riehle, Department of Computer Science

The automation of software development, to increase efficiency of the development effort and improve the software product, has long been a goal of software engineering. This efficiency (high productivity with less software faults) results from best practices in building, managing and testing software projects via the use of these automated tools and processes. However, each software development tool has its own characteristics, semantics, objects, and concepts. While there have been significant results achieved by use of automated software development tools (coming mainly from the widespread increase of customers' adoption of these tools), there remain many challenging obstacles: lack of communication between the different software development tools, poor shared understanding; use of different syntax and concepts between tools, limit of interoperability between tools, absence of unifying conceptual models and ideas between tools, and redundant work and cross purposes between tools.

The approach undertaken to overcome some of these obstacles was to construct a "pilot" ontology that might be extended in the future to include other software development tools. The Feature-Oriented Domain Analysis approach was applied to capture the commonalities between two software development tools, Rational Software Corporation's Requisite®Pro (a main-stream, complex, commercial tool) and a software prototyping tool, the Software Engineering Automation tool or SEA Tools (a research model with tool support for developing executable software prototypes). An ontology was developed for the software development tools using the Protégé-2000 System. The ontology, expressed in UML, promotes interoperability and enhanced communication.

KEYWORDS: Software Engineering, Computer Science, Management, Ontologies

SIMPLE NETWORK MANAGEMENT PROTOCOL OVER WI-FI WIRELESS NETWORKS

Jiradett Kerdsri-Lieutenant, Thai Air Force
B.E., Thai Air Force Academy, 1998
Master of Science in Computer Science-March 2003
Advisor: Ted Lewis, Department of Computer Science
First Reader: Geoffrey Xie, Department of Computer Science
Second Reader: Gurminder Singh, Department of Computer Science

Simple Network Management Protocol (SNMP) allows users of network equipment (i.e., network administrators) to remotely query the state of any device being tested for system load, utilizatinon and configuration. Windows NT, Windows 2000 and Windows XP Professional are all equipped with SNMP service so that an SNMP manager can communicate with an SNMP agent running on a wireless 802.11b client. However, the rest of Windows operating systems, including Windows CE and Pocket PC, have to run third party proxy SNMP agents in order to be recognized by an SNMP management application.

This thesis describes an implementation of a Pocket PC SNMP agent for two Pocket PC mobile devices accessing a wired network via an 802.11b wireless link. As a result of the implementation performed in this thesis, an SNMP manager can wirelessly communicate with a Pocket PC client. However, other results found that only some of the commercially available SNMP managers are able to access the mobile SNMP client and its management information base, due to incompatible implementations of the server and client software.

KEYWORDS: Pocket PC, IEEE 802.11b, Wireless Network, SNMP, Windows CE 3.0, PDA, MIB, ActiveX, IPWorks!

DISTRIBUTED ARCHITECTURE FOR THE OBJECT-ORIENTED METHOD FOR INTEROPERABILITY

George M. Lawler-Lieutenant, United States Navy
B.S., United States Naval Academy, 1995
Master of Science in Computer Science-March 2003
Advisor: Valdis Berzins, Department of Computer Science
Second Reader: CAPT Paul E. Young, USN, Department of Computer Science

The Department of Defense (DoD) is both challenged by the quest for interoperability and capable of the bottom-up development of a solution. The predominant method for achieving interoperability is the development of an intermediate representation that provides a common integration language or data model. An example is Young's Object-Oriented Method for Interoperability (OOMI), which produces a Federation Interoperability Object Model (FIOM) for the resolution of heterogeneities in representation and view of a real-world entity. An FIOM generates a standard for interoperability by associating the non-standard, component system data models into an extensible lattice, which captures translations that resolve data modeling differences. To support the bottom-up creation of an FIOM, this thesis: (1) describes a self-similar approach to data storage that allows generic data structures to be manageable, extensible and asynchronously populated, and (2) introduces a lattice concept for facilitating efficient and scalable object inheritance relationships. It is asserted that DoD's acquisition environment necessitates a distributed approach to solving the interoperability challenge. The description of a distributed software system to facilitate the collaborative construction of an FIOM within the existing DoD structure, and provide an architecture to guide the development of such a distributed collaborative environment, is presented.

KEYWORDS: Interoperability, Object-Oriented Method for Interoperability, Distributed Systems, Collaboration, Self-Similar Data Structures, Lattice Concept, FIOM Lattice, Peer Networking, XML, Data Binding, Layered Architecture, Distributed OOMI

USING XML/HTTP TO STORE, EDIT, SERVE, AND ANNOTATE TACTICAL SCENARIOS FOR X3D OPERATIONAL VISUALIZATION AND ANTI-TERRORIST TRAINING

Khaled Mnif-Captain, Tunisian Army
B.S., FSEG Sfax, 1985
Master of Science in Computer Science-March 2003
Advisors: Don Brutzman, Department of Information Science
Curtis L. Blais, Modeling, Virtual Environments, and Simulation Institute

Adopting Extensible Markup Language (XML) and Hypertext Transfer Protocol (HTTP) are key steps to accommodate the evolution of Internet technologies. While HTTP is already a proven standard communication protocol responsible for the rapid expansion of the World Wide Web, XML provides general mechanisms for determining validatable documents and addresses several deficiencies of HTML regarding diverse document structure and content. XML and HTTP together provide many of the essential capabilities associated with database engines

XML enables the creation of web documents that preserve data structure and simultaneously provide human-readable and machine-readable information to facilitate web automation. Today XML can guarantee platform-independent inter-application data interchange. XML is becoming an enabling technology on the Internet, transforming the Web from a static medium to a powerful infrastructure for collaborative and interoperable applications.

The Modeling, Virtual Environments and Simulation (MOVES) Institute of the Naval Postgraduate School (NPS) is continuing to build a database of 3D tactical scenarios and using X3D and VRML tools. The configuration parameters and statistical results of these scenarios are XML documents. For better understanding and usability of these results by the end users, a Web-based application stores and manipulates these XML documents.

This thesis develops a server-side application that can store, serve, and annotate tactical scenarios for X3D operational visualization and anti-terrorist training by using XML and HTTP technologies. The experimental demonstration for this work is the prototypical Anti-terrorism/Force Protection (AT/FP) simulation model developed by Lieutenant James W. Harney, USN, using Extensible 3D Graphics (X3D)/ Virtual Reality Modeling Language (VRML) models.

KEYWORDS: Extensible Markup Language, XML, Hypertext Transfer Protocol, HTTP, Extensible 3D Graphics, X3D, Extensible Stylesheet Language Transformations, XSLT, Scalable Vector Graphics, SVG, Force Protection, Anti-terrorism, SAVAGE

HOW INTRUSION DETECTION CAN IMPROVE SOFTWARE DECOY APPLICATIONS

Valter Monteiro, Jr.-Lieutenant Commander, Brazilian Navy
B.S., Universidade de Sao Paulo, 1994
Master of Science in Computer Science-March 2003
Advisor: Neil C. Rowe, Department of Computer Science
Second Reader: J.D. Fulp, Department of Computer Science

This research concerns information security and computer-network defense. It addresses how to handle the information of log files and intrusion-detection systems to recognize when a system is under attack. The goal is not the usual one of denying access to the attacker, but rather providing a justification for deceptive actions to fool the attacker. A simple demonstration of how two different kinds of open-source intrusion-detection systems can efficiently pool data for this purpose was implemented.

KEYWORDS: Intelligent Software Decoy, Intrusion Detection, Computer Deception, Response Mechanism, Log File Monitor

EVALUATION OF SECURE 802.1X PORT-BASED NETWORK ACCESS AUTHENTICATION OVER 802.11 WIRELESS LOCAL AREA NETWORKS

Huseyin Selcuk Ozturk-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1997
Master of Science in Computer Science-March 2003
Advisor: Geoffrey Xie, Department of Computer Science
Second Reader: John Gibson, Department of Computer Science

Since wireless technology has been used in Local Area Networks (LAN), our networks are easier to build and are more scalable and mobile than legacy structures. While providing these functionalities, Wireless LANs (WLAN) have some security vulnerabilities that should be addressed. Failing to examine the security risks of WLAN technology and take the necessary countermeasures may result in unauthorized entry into the legacy local area networks and other attacks. A secure connection to an intranet, which holds critical data and applications, must be the utmost consideration in the effort to protect critical resources. This thesis builds an open source test-bed for evaluating WLAN security protocols. Moreover, it investigates the suitability of the IEEE 802.1X standard to provide the required security framework to WLANs. This research determines that the IEEE 802.1X could enhance the security level in authentication and privacy by the enabling rekeying process, but would not prevent Denial of Service attacks via unauthenticated management frames.

KEYWORDS: Wireless Local Area Networks, Security, User Authentication Base, Threat Model for Critical Infrastructures, Organizational Security Policy for Wireless LAN, EAP-TLS Authentication Method

DESIGN AND TEST OF THE CROSS-FORMAT SCHEMA PROTOCOL (XFSP) FOR NETWORKED VIRTUAL ENVIRONMENT

Ekrem Serin-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1997
Master of Science in Computer Science-March 2003
Advisors: Don Brutzman, Department of Information Science
CDR Joseph A. Sullivan, USN, Department of Computer Science

A Networked Virtual Environment (Net-VE) is a distributed software system in which multiple users interact with each other in real time even though these users may be located around the world [Zyda 99]. Net-VEs first gained attention through a variety of DOD and academic research projects. After release of the multiplayer game DOOM, the gaming industry captured the idea of interactive multiplayer games. Today there are many popular Internet-based multiplayer games available.

Effective networking of diverse entities and systems is a common problem for Networked Virtual Environments. In order to communicate with other entities, a variety of communication protocols are used. Historically these communication protocols are "hard coded" into the software system and all nodes that participate in the environment must identically implement the protocols to interact with others. These communication protocols require authoring and compiling by a trained programmer. When the compiling process is introduced to the networked virtual environment, it detracts the extensibility and dynamicism of the system.

This thesis presents the design and development of a Networked Virtual Environment model that uses Cross Format Schema Protocol (XFSP). With this work, it is shown that a networked simulation can work for 24 hours a day and seven days a week with an extensible schema based networking protocol and it is not necessary to hard code and compile the protocols into the networked virtual environments. Furthermore, this thesis presents a general automatic protocol handler for a schema-defined XML document or message. Additionally, this work concludes with idea that protocols can be loaded and extended at runtime, and can be created with different-fidelity resolutions, resulting in swapping at runtime based on distributed state.

KEYWORDS: Networked Virtual Environments, Cross Format Schema Protocol (XFSP), XML, XSD, SOAP, HLA, NPSNET-V, JXTA, XML Serialization

REDEFINING ATTACK: TAKING THE OFFENSIVE AGAINST NETWORKS

Zachary H. Staples-Lieutenant, United States Navy
B.S., United States Naval Academy, 1995
Master of Arts in National Security Affairs-March 2003
Robert J. Michael, II-Lieutenant, United States Navy
B.S., Texas A&M University, 1994
Master of Science in Modeling, Virtual Environments, and Simulation-March 2003
Master of Science in Computer Science-March 2003
Advisors: Daniel Moran, Department of National Security Affairs
Rudolph P. Darken, Department of Computer Science
John Hiles, Department of Computer Science

The Information Age empowers individuals and affords small groups an opportunity to attack states' interests with an increasing variety of tactics and great anonymity. Current strategies to prevail against these emerging threats are inherently defensive, relying on potential adversaries to commit mistakes and engage in detectable behavior. While defensive strategies are a critical component of a complete solution set, they cede initiative to the adversary. Moreover, reactive measures are not suited to quickly suppress adversary networks through force. To address this shortfall in strategic planning, the science of networks is rapidly making clear that natural systems built over time with preferential attachment form scale-free networks. These networks are naturally resilient to failure and random attack, but carry inherent vulnerabilities in their highly connected hubs. Taking the offensive against networks is therefore an exercise in discovering and attacking such hubs. To find these hub vulnerabilities in network adversaries, this thesis proposes a strategy called Stimulus Based Discovery, which leads to rapid network mapping and then systematically improves the accuracy and validity of this map while simultaneously degrading an adversary's network cohesion. Additionally, this thesis provides a model for experimenting with Stimulus Based Discovery in a Multi-agent System.

KEYWORDS: Information Age Warfare, Information Superiority, Stimulus Based Discovery, Targeting, Multi-agent Systems, Complex Adaptive Systems, Relationships, Networks, Connectors, Tickets, Simulation, Network Centric Warfare, Counter Terrorism, Strategy

A GENERIC ARCHITECTURE FOR DECEPTION-BASED INTRUSION DETECTION AND RESPONSE SYSTEM

Engin Uzuncaova-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1997
Master of Science in Computer Science-March 2003
Master of Science in Software Engineering-March 2003
Advisors: J. Bret Michael, Department of Computer Science
Richard Riehle, Department of Computer Science

Today, intrusion detection systems provide for detecting intrusive patterns of interaction. Although the responses of such systems are typically limited to primitive actions, they can be supplemented with deception-based strategies. This thesis proposes a generic software architecture combining intrusion detection and deceptive response capabilities in a uniform structure. Detecting and responding to attacks are realized via runtime instrumentation of kernel-based modules. The architecture provides for dynamically adjusting system performance to maintain continuity and integrity of both legitimate services and security activities.

KEYWORDS: Computer Security, Intrusion Detection, Intrusion Response, Deception, Software Architecture, Unified Modeling Language